FORTINET®

Fighting Cybercrime with Artificial Intelligence

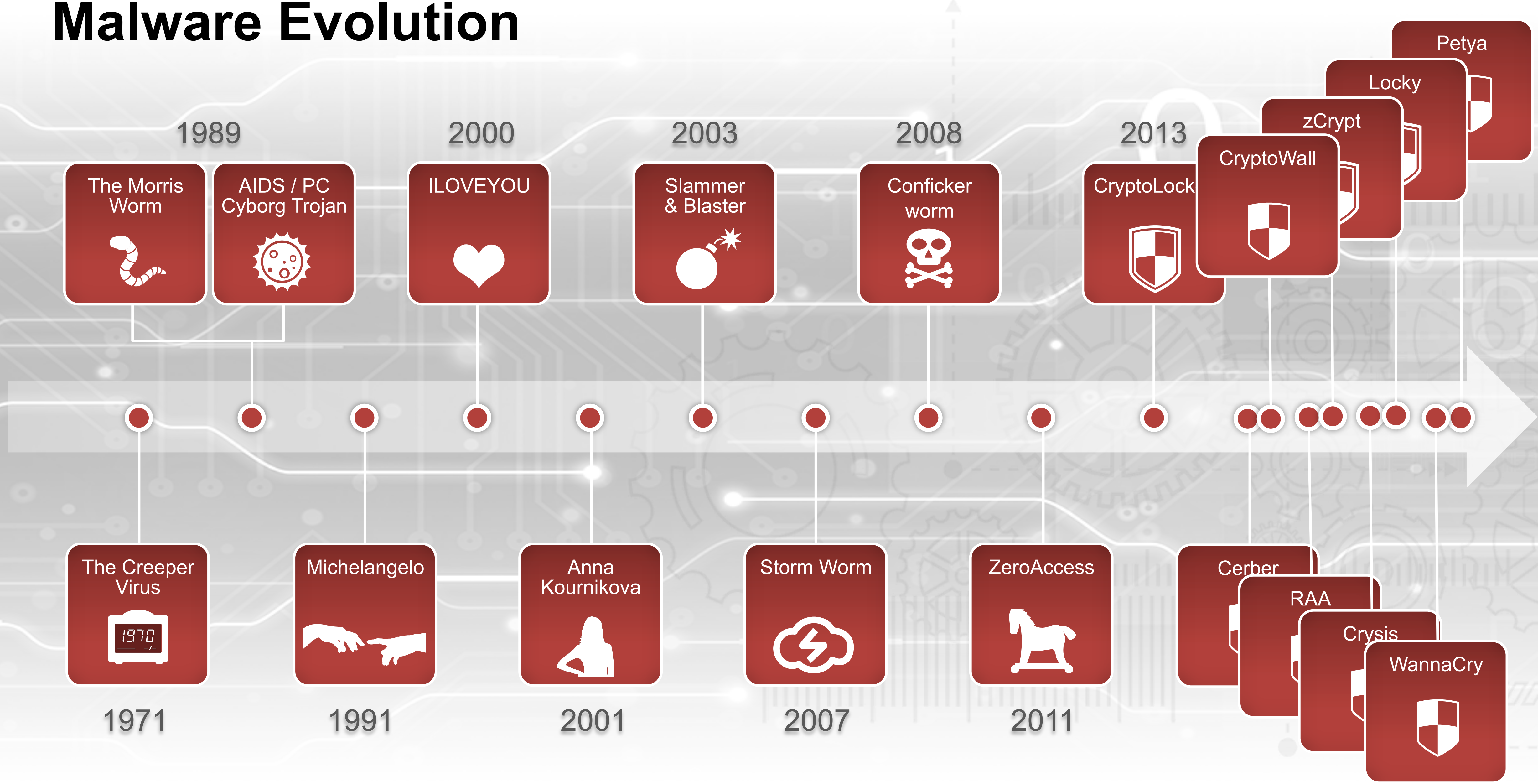
Peter Kocik, Systems Engineer CEE

June 29, 2018

© Copyright Fortinet Inc. All rights reserved.

```
Dis is one half.
Press any key to continue…
```

Malware Evolution



Ransomware as a service

What We're Up Against - RaaS in an Hour

10.00pm

10.30pm

10.45pm

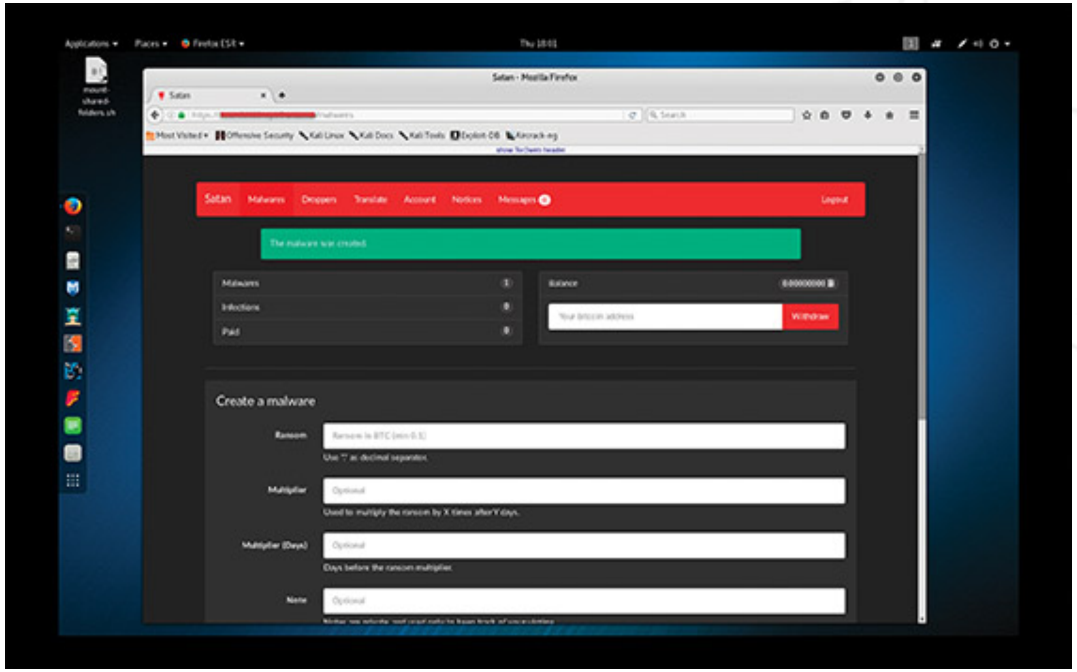
11.00pm

10.05-10.44pm
Locate and setup a VPN service to hide your IP address

10.44-10.58pm
Connect to the Satan website on the Dark Web

11.01pm
Ransomware created using a simple dashboard
Commission based fee structure – commission charged reduces depending on the number of infections and payments

11.04pm
Ransomware downloaded as an executable, ready to be distributed
Checked against VirusTotal – no match



The malware was created.

Malwares 1
Infections 0
Paid 0

Balance 0.00000000

Your bitcoin address

Create a malware

Ransom: Ransom in BTC (min 0.1)
Use "." as decimal separator.

Multiplier: Optional
Used to multiply the ransom by X times after Y days.

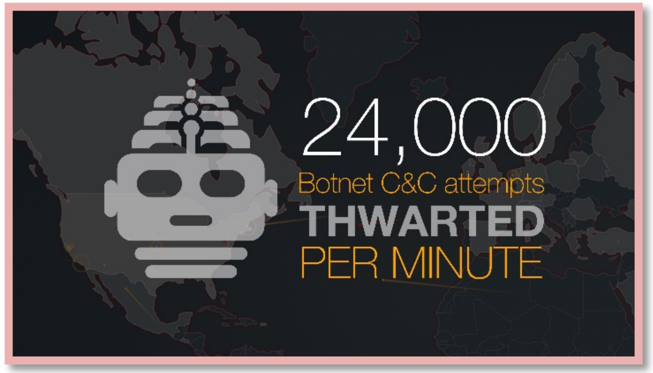
Multiplier (Days): Optional
Days before the ransom multiplier.

Note: Optional

"I signed up on the website and didn't even need an email address. The company takes a 30 per cent cut and I get 70 per cent. I don't think that's too bad, and if I didn't like it I'd just charge more for my ransomware!"

https://www.channelweb.co.uk/crn-uk/feature/3008586/how-to-launch-a-ransomware-attack-in-less-than-an-hour

Our threatresearch by the numbers



24,000
Botnet C&C attempts
THWARTED
PER MINUTE

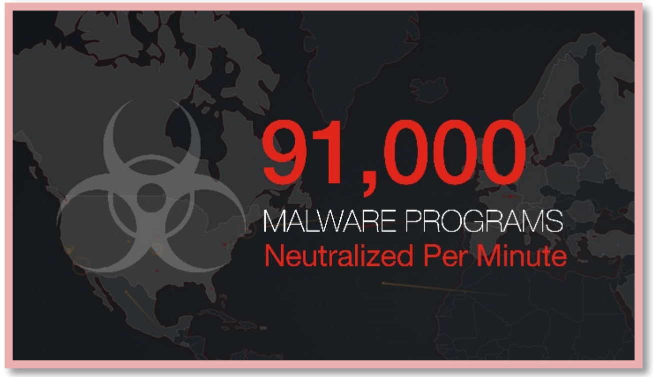
150,000
Malicious Website
ACCESSES Blocked Per Minute

500
ZERO DAY
THREATS DISCOVERED

100
INTRUSION
PREVENTION
RULES PER WEEK

4,400,000
NETWORK INTRUSION
ATTEMPTS
resisted per minute

415 TB of Threat Samples



91,000
MALWARE PROGRAMS
Neutralized Per Minute

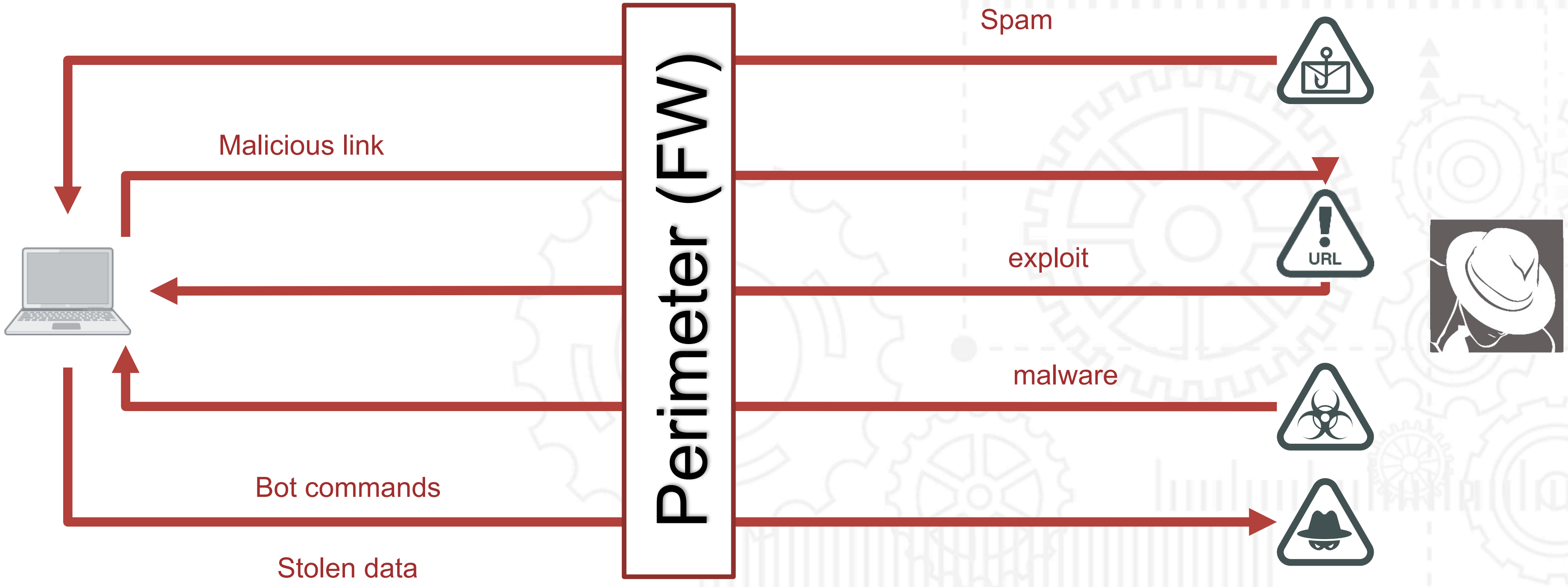
450,000 HOURS of Threat Research
GLOBALLY PER YEAR

21,000
INTRUSION
PREVENTION
RULES

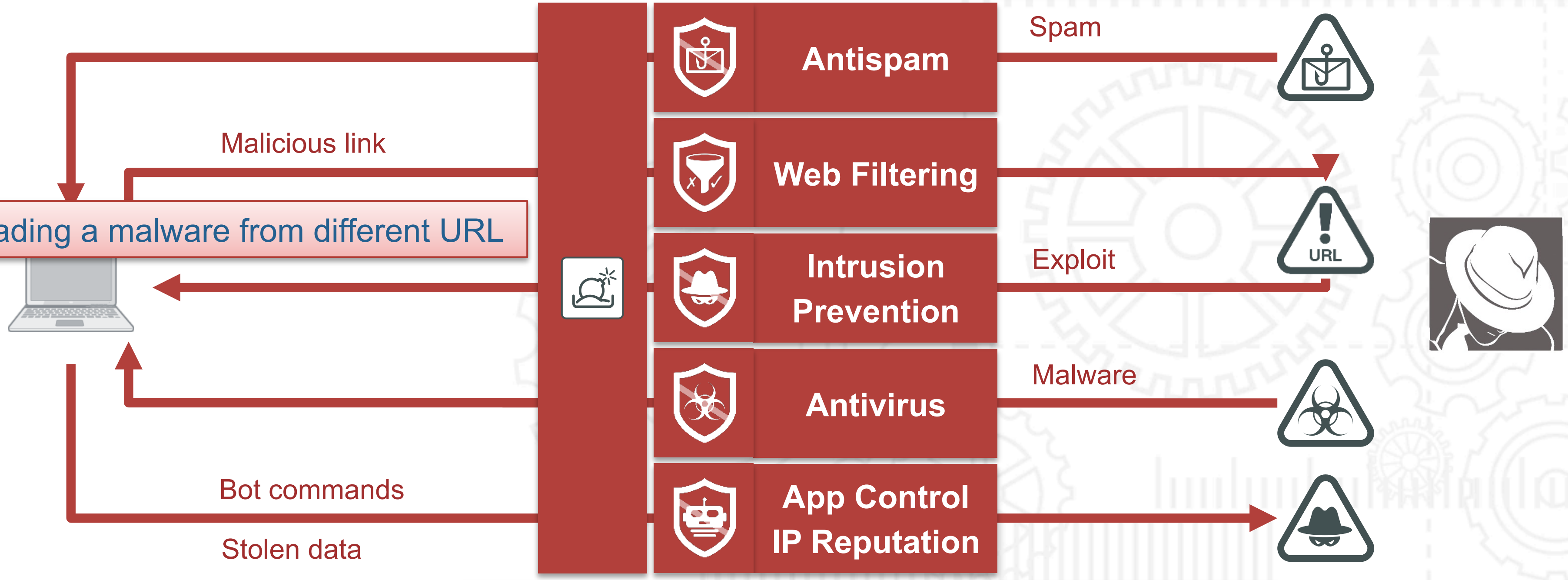
50,000,000,000 +

Events Ingested Daily

Typical attack used today



Typical attack used today



Email with link pointing to an compromised web page

Java script which is downloading a malware from different URL

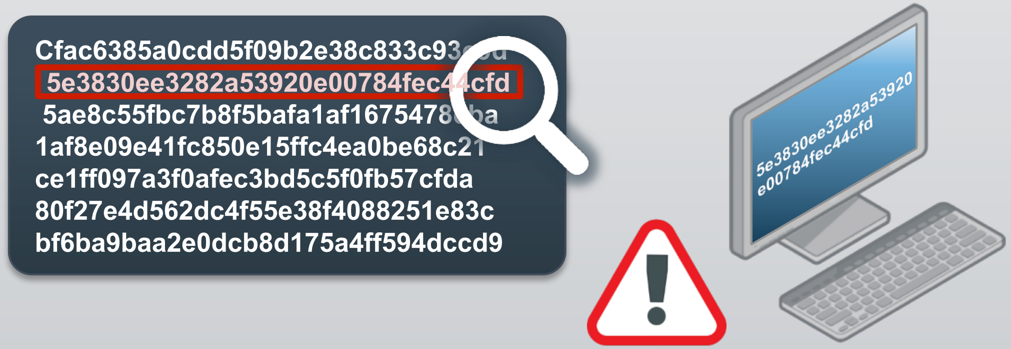
ALL URL/DNS/IPs reputation scores were ‘unknown’ or ‘clean’

Antivirus Evolution

LEVEL I

- Simple MD5 / SHA 56 computations
- Resulted in large DBs for file comparisons
- One signature – one piece of malware
- Reactive and non-responsive to mutations

```
C:\Md5sum malware.exe
5e3830ee3282a53920e00784fec44cfd (malware.exe)
```

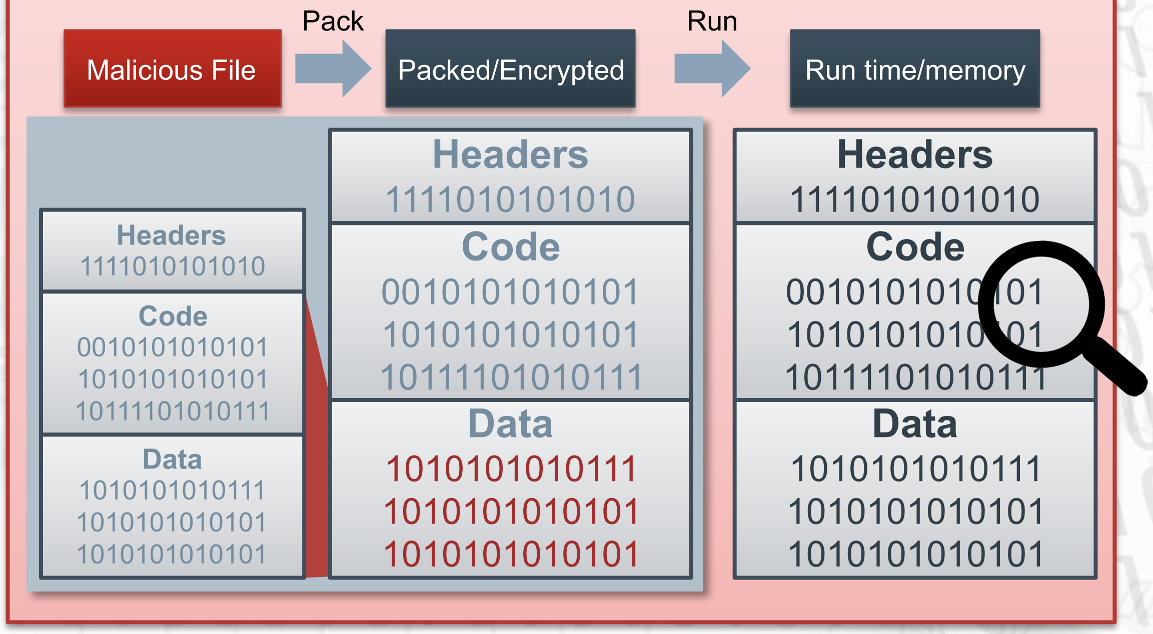


```
Cfac6385a0cdd5f09b2e38c833c93[illegible]
5e3830ee3282a53920e00784fec44cfd
5ae8c55fbc7b8f5bafa1af1675478[illegible]ba
1af8e09e41fc850e15ffc4ea0be68c21
ce1ff097a3f0afec3bd5c5f0fb57cfda
80f27e4d562dc4f55e38f4088251e83c
bf6ba9baa2e0dcb8d175a4ff594dccd9
```

Malware Found

LEVEL II

- Content Pattern Recognition Language
- Looks at wrappers and payload for repeats
- Handles large volumes of permutations
- Proactive in nature



Malicious File → Pack → Packed/Encrypted → Run → Run time/memory

Malicious File:

Headers
1111010101010

Code
0010101010101
1010101010101
1011110101011

Data
1010101010111
1010101010101
1010101010101

Packed/Encrypted:

Headers
1111010101010

Code
0010101010101
1010101010101
1011110101011

Data
1010101010111
1010101010101
1010101010101

Run time/memory:

Headers
1111010101010

Code
0010101010101
1010101010101
1011110101011

Data
1010101010111
1010101010101
1010101010101

Early AI Defined

Alan Turing called an infant's mind an 'unorganized machine' in 1930s

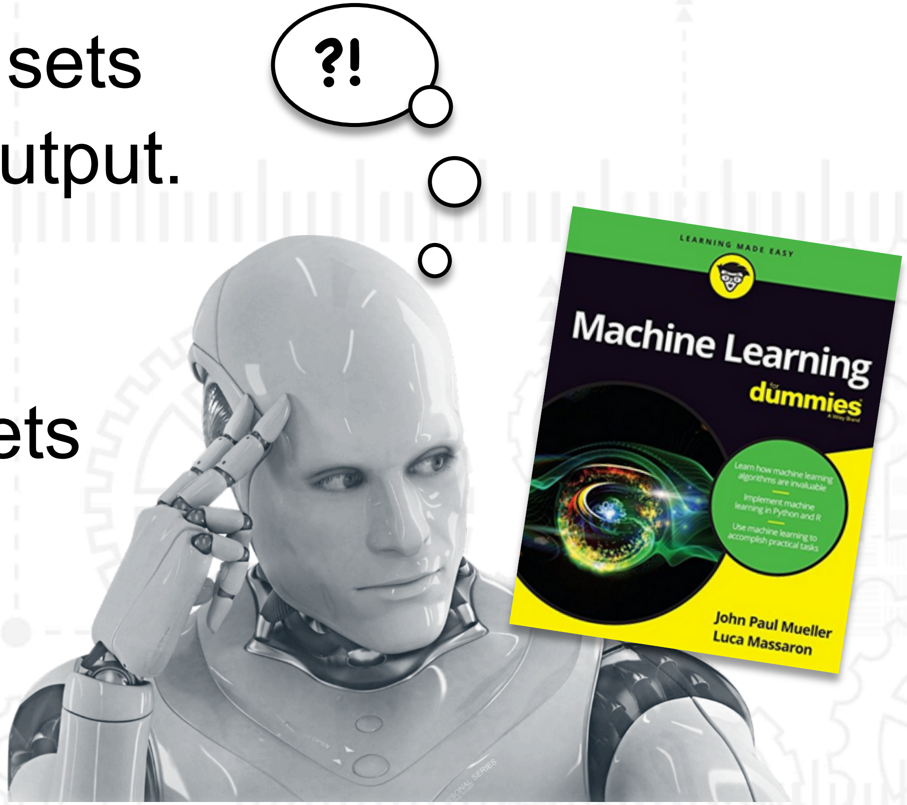
Created early definitions of machine learning

- First type (A) consists of simple NAND (negative – AND gates
- Second type (B) is combination of A types with modifiers added – results in weighted input/variable output method
- Saw the need for:
  - **Seeded solution set of accurate or known potential output**
  - **Population of variably weighted pieces or functions**
  - **A method for removing the worst solutions while retaining the best**

Major inhibitor of his research – was far ahead of available capabilities in terms of computing power.

Types of Problem Solving

- **Supervised Learning** – Using known solution sets to embed proper functions and create proper output.
  - **Reinforcement** – action on an environment triggers an observation resulting in a defined state.
- **Unsupervised** Learning – unknown solution sets
  - **Clustering** – group according to similarities.
  - **Dimensionality Reduction** – deductive reasoning.
  - **Structured Prediction** – random fields are analyzed to predict according to defined output probabilities.
  - **Anomaly Detection** – input does not match expectations.

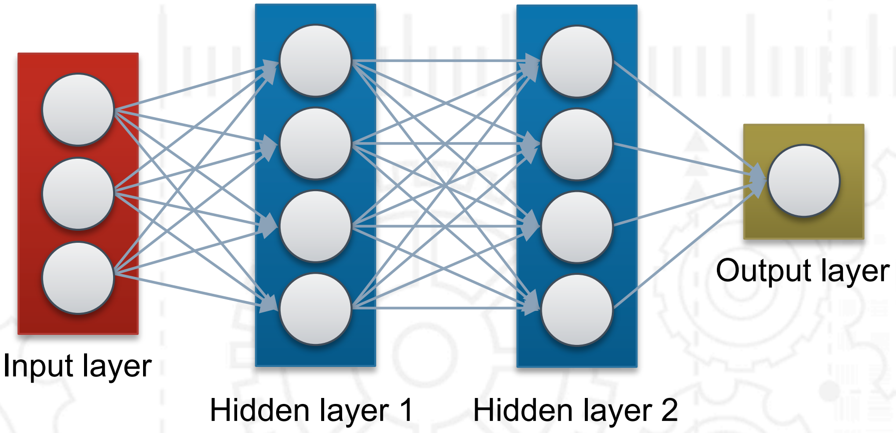


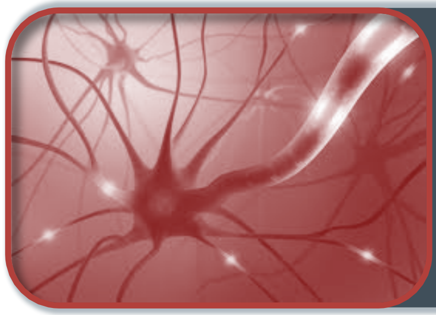
Artificial Neural Networks (ANNs)
Large collections of simple interconnected nodes (neurons), each with a weighted input and output value.

Type of AI – Artificial Neural Network (Multilayer Perceptron)

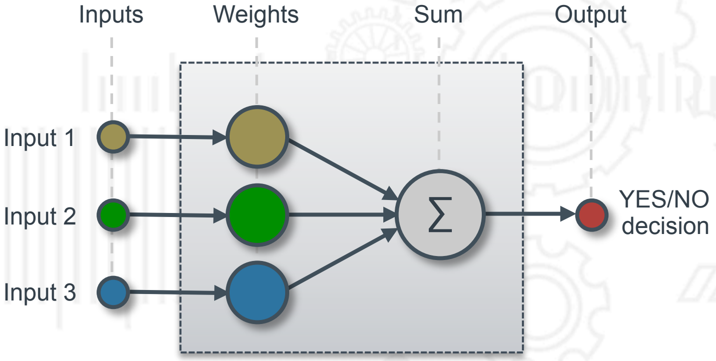
- Consists of three or more layers
  - » Input layer
  - » One or more hidden layers
  - » Output layer
- Layers are made of up nodes
  - » Connected to every node in the previous and subsequent layer
  - » Provide discrete processing of input information (files and features)
  - » Produces an output value based on inputs, function, and weighted valuation

The Multilayer Perceptron approach provides deep machine learning capabilities.





MP behavior is similar to human neurons - if input is strong enough, signal is passed according to weighted value



Features

- Point observable characteristics
- 1 : 1 relationship with nodes
- Features are maintained in a knowledgebase repository
- Quality is critical
  - » Provides more accurate determination of file status
  - » Fortinet AI leverages internal legacy samples (~.5PB) to create features from samples
- Each feature is weighted to assist in decisions
- Feature weighting can change over time
- Weighted features are processed within nodes
  - » Output is weighted, based on presence of features
  - » Weighted output passed to next layer for continued processing

Feature/Node Algorithm

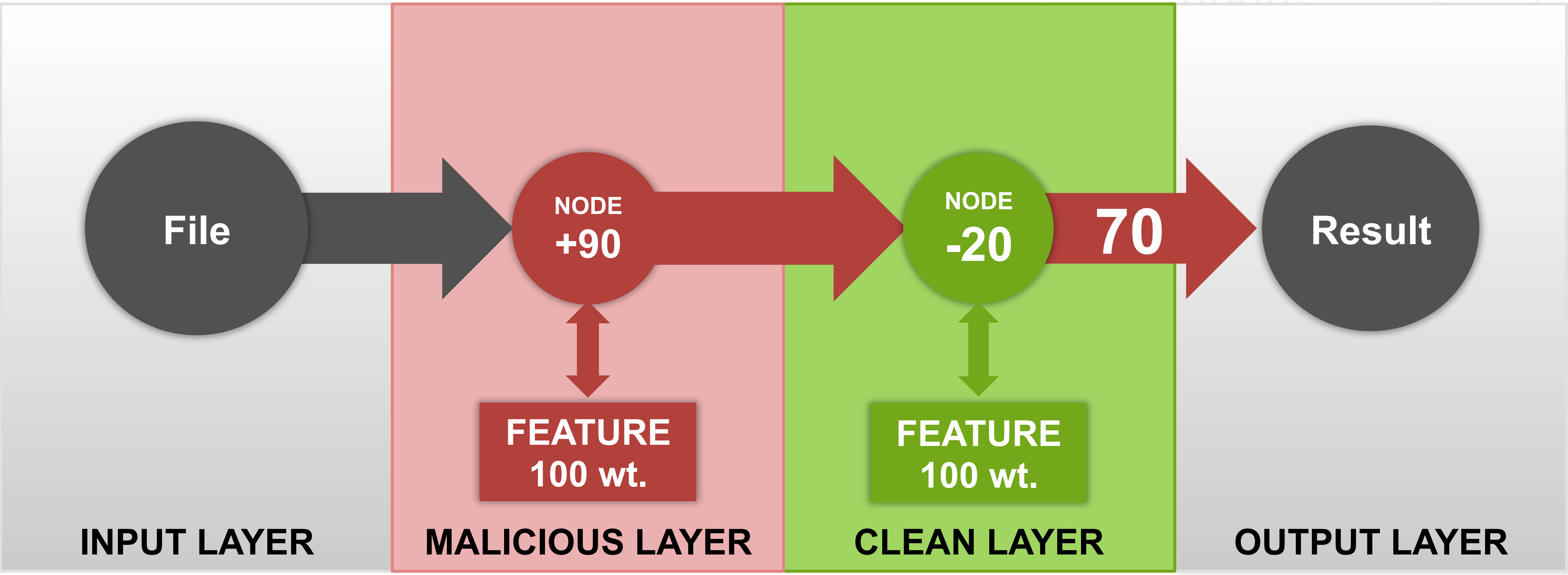
f - feature

w - weight

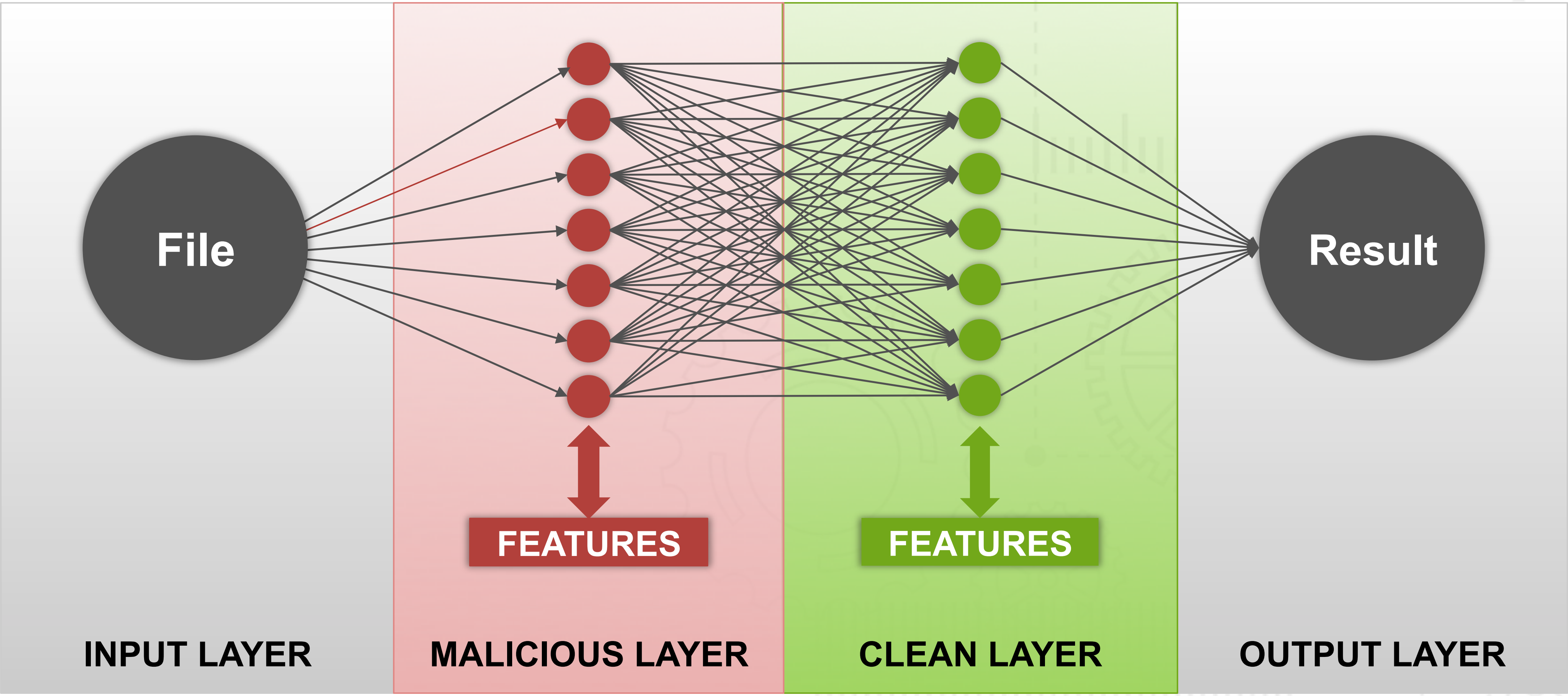
Func(f1*w1+f2*w2+...+fn*wn) -> {0,1}

Features, Nodes & Weights – Single Instance

1. We start with an input file – malicious or clean
2. Feature presence is calculated, re-weighted and passed forward to the next node
3. The analysis is repeated using the next layer feature, then passed to the next node
4. Result – the overall probability based on a score of feature presence

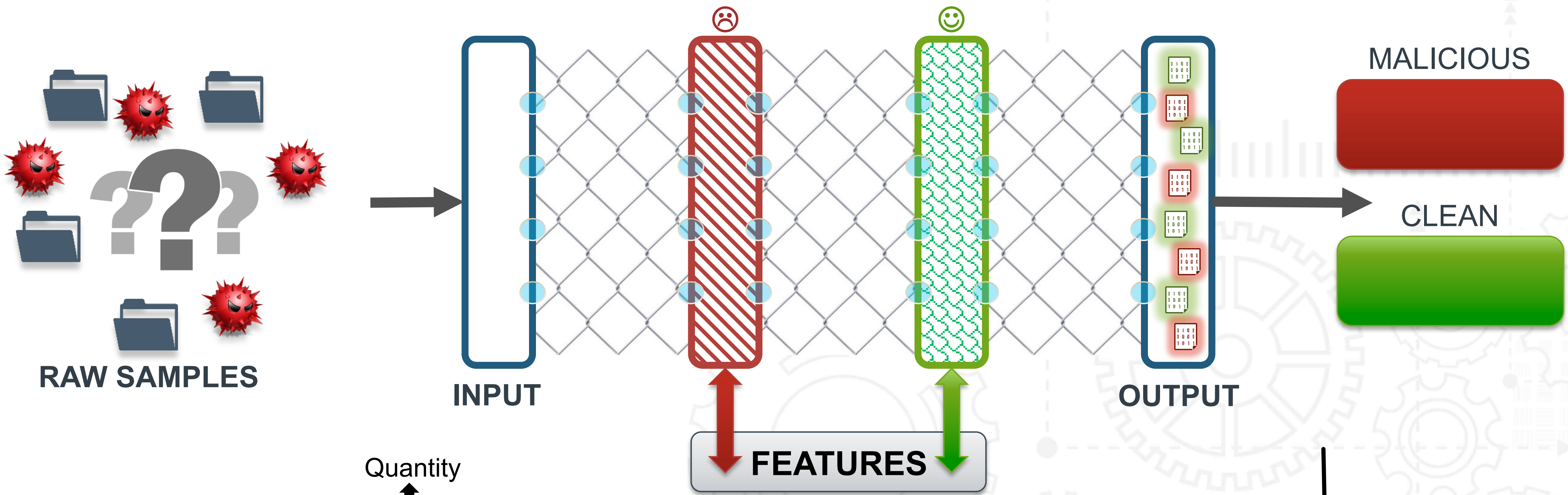


Features, Nodes & Weights – Multiple Instance



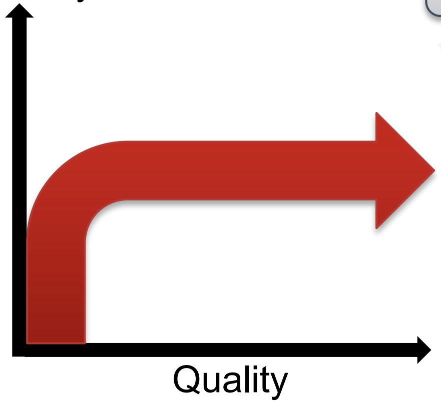
Output is a result of 2.3B x 3.3B individual node computations.

FortiGuard AI in Operation

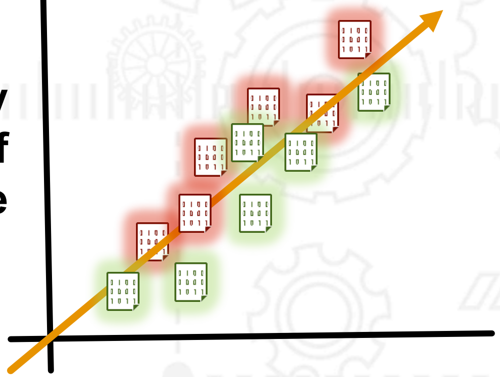


Feature Set Improvements

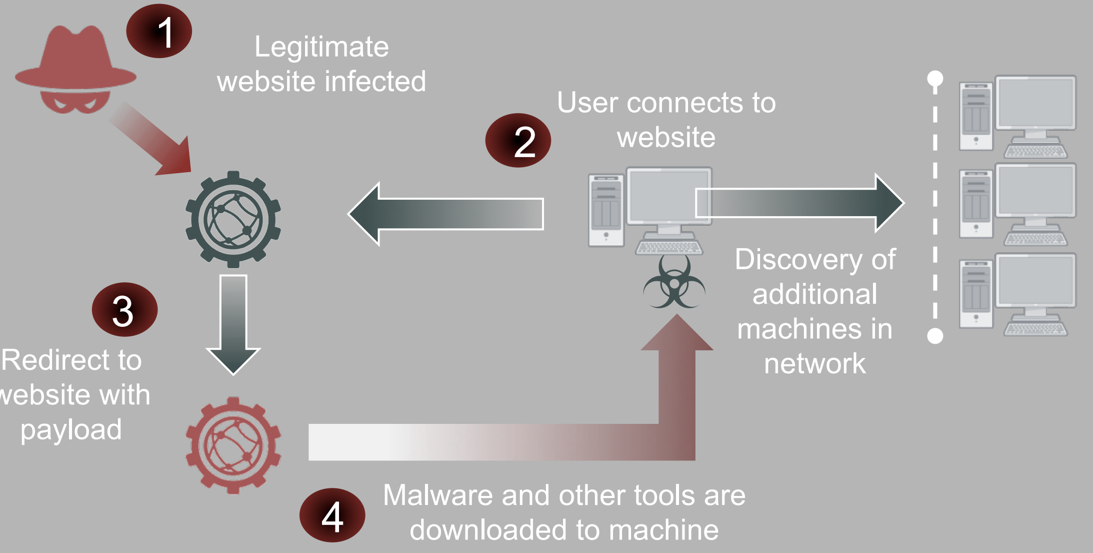
- Quality
- Stabilized Number
- Weighting Confidence

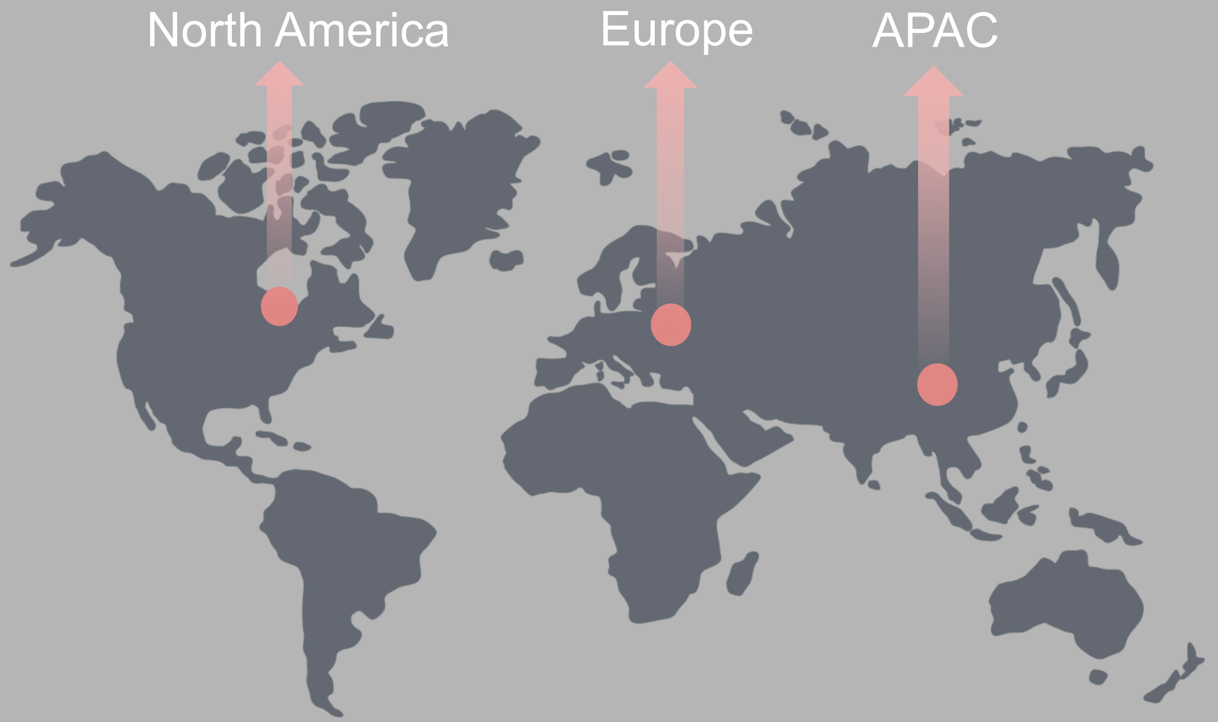


Continued Accuracy to a High Degree of Confidence



RATANKBA Malware – Global Attack Campaign


1
Legitimate website infected
2
User connects to website
3
Redirect to website with payload
Discovery of additional machines in network
4
Malware and other tools are downloaded to machine



Prior Dates: Fortinet's Machine-Learning methods analyze millions of files thru a sophisticated neural-network discovering new zero-days and malware variants.

Oct 29th. 2016: Fortinet's machine-to-machine defensive system releases dynamic algorithm (W32/ Generic.AC.39AB6D!tr)

Feb 8th, 2017: Trend Micro discloses RATANKBA malware. Fortinet customers are proactively protected based on Oct 2016 algorithm.

Feb 9th. ,2017: Symantec releases additional hash information on RATANKBA which Fortinet is already blocking based on Oct 2016 algorithm.

Feb 10th ,2017: Fortinet discovers several malicious domains. Customers are protected through web filtering and DNS engines.

Feb 14th, 2017: Several additional domains are published and determined to be part of RATANKBA malware which Fortinet had protection 4 days prior..

FORTINET®